

6 4 8 1 4 . 0 2 1 2

System and Method for Wireless Audit and Cashless Transaction Transport

Inventor: Erin M. Defossé
11005 Plumewood Drive
Austin, Texas 78750

CROSS REFERENCE TO RELATED APPLICATIONS

This application (a) is a continuation-in-part of U.S. Patent Application Serial No. _____ filed on _____ and entitled "*System and Method for Auditing a Vending Machine*" (attorney docket no. 064814.0212), which (b) is a continuation-in-part of U.S. Patent Application Serial No. 09/971,170 filed on October 4, 2001, and entitled "*Remote Data Acquisition, Transmission and Analysis System Including Handheld Wireless Equipment*" (attorney docket no. 064814.0184), which (c) is a continuation-in-part of U.S. Patent Application Serial No. 09/267,254 filed on March 12, 1999 by Erin M. Defossé entitled "*A Wide Area Network Operation's Center that Sends and Receives Data from Vending Machines*," now U.S. Patent No. 6,457,038, which claims priority to (d) U.S. Provisional Patent Application Serial No. 60/078,645, filed March 19, 1998, and entitled "*Remote Data Acquisition and Transmission System for the Monitoring and Control of Vending Machines*," and (e) U.S. Provisional Patent Application Serial No. 60/099,434, filed September 8, 1998, and entitled "*Remote Data Acquisition and Transmission System*;" and this application claims priority to U.S. Provisional Patent Application Serial No. _____, filed _____, and entitled "*System and Method for Wireless Audit and Cashless Transaction Transport*."

Assignee: Isochron Data Corporation
6801 Capital of Texas Highway
Building 2, Suite 200
Austin, Texas 78731

BAKER BOTTS L.L.P.
1600 San Jacinto Center
98 San Jacinto Blvd.
Austin, Texas 78701-4039

Attorney Docket: 064814.0214

BEST AVAILABLE COPY

Product Requirements Document

Project: Glaux 2.0

Product Requirements Document

VendCast Audit Device

Project Name: Glaux



DRAFT

Document Version:	DRAFT 2.0b11
Date:	13-Nov-2002
Author:	Erin Defosse

Product Requirements Document

Project: Glaux 2.0

Document Control:

Version	Date	Author	Description
1.0a1	08-Apr-2002	E. Defosse	Initial Draft Release
1.0b1	09-Apr-2002	E. Defosse	Renamed document as a "Product Requirements Document" and added various details in the Detailed System Requirements section. Document is fairly complete now.
1.0b2	22-Apr-2002	E. Defosse	Made changes based on in-house review done on 18-Apr-2002. Major changes included: 1) removing requirement of having the AD know how to write Vendor Asset Info to the VMC leaving it to the handheld to compose the required DEX and only requiring that the AD push the DEX to the VMC, 2) Divided the Install use case into two (one with a handheld, the other without a handheld), 3) Only required that AD (in Phase 1) work with cold drink vendors, 4) Removed Vendor Information data as explicit data fields and rolled it into the Ad-Hoc data.
1.0	23-Apr-2002	E. Defosse	Made small editorial changes to 1.0b2 and published as final doc (v 1.0). Added more detailed milestones and deliverable dates.
2.0b1		E. Defosse	New version of Glaux that uses Bluetooth as comms mechanism. Also incorporates an electronic lock interface.
2.0b2-b6		E. Defosse	Miscellaneous editorial changes. 2.0b6 released to TenX to start development.
2.0b7	24-Sep-2002	E. Defosse	Made AES encryption and SHA-1 hashing a MUST requirement. Defined details of electronic lock interface (power, # pins, etc.). Added details on authentication and security model between Glaux and Handheld and referred the reader to the Glaux Security PRD for details. Added requirement for a SAM to store encryption keys. Added encryption keys and domain hierarchy to information architecture. Clarified Bluetooth security section to include a PIN. Tightened power output requirement on expansion bus to match filtered power

Product Requirements Document

Project: GlauX 2.0

			provided to electronic lock. Made Widcomm Bluetooth stack a MUST requirement.
2.0b8	23-Oct-2002	E. Defosse	<p>Changes to detailed requirements:</p> <p>PAN</p> <ol style="list-style-type: none"> 1) The Asset ID of the vending machine will be used as the BT name instead of the Outlet ID. 2) Will use the unique manufacturing serial number as the default BT name <p>Security</p> <ol style="list-style-type: none"> 1) Added PKI capabilities and the need to store the Agent's key pair and the host's public key 2) Specified exact number and type of AES keys loaded at manufacture <p>Hard Reset</p> <ol style="list-style-type: none"> 1) Never delete the (E-lock) Access Log when doing a Hard Reset 2) Never delete the Handheld, General Events logs when doing a Hard Reset 3) Only clear DEX and MDB Archives when doing a Hard Reset 4) Set all config parameters to factory defaults when doing a Hard Reset 5) Never clear the time reference when doing a Hard Reset <p>Soft Reset</p> <ol style="list-style-type: none"> 1) Equivalent to rebooting 2) Nothing is cleared <p>Deleting the Access Logs, Handheld log, and Gen Events logs could be accomplished through a specific command in the protocol and not through a reset process.</p> <p>Removed development milestones section.</p>
2.0b9	1-Nov-2002	E. Defosse	Corrected error in meaning of "Install Flag" so that Install Flag = True implies that ALL security is turned off (both Bluetooth and App Level)
2.0b10	7-Nov-2002	E. Defosse	Added "Has DEX Port" and "Lock Installed"

Product Requirements Document

Project: Glaux 2.0

			configuration parameters Changed "default" Bluetooth Name to be "ISO" prepended to the Audit Device's manufacturing serial number, if no serial number is present then Bluetooth Name further defaults to "ISO" prepended to the MAC address of the Bluetooth transceiver
2.0b11	13-Nov-2002	E. Defosse	Added requirement that "Lock Installed" flag be overridden and set to True if Audit Device determines that a lock is present. Replaced "ISO" prefix used in Bluetooth name with "HIAD" prefix.

Approvals:

Who	Company	Signature	Date

Product Requirements Document

Project: Glaux 2.0

1 Introduction

The purpose of this document is to detail the set of features required for the *VendCast Audit Device*, herein called *Glaux*. This project's goal is to develop an embedded data collection and storage device that, when placed in inside a vending machine, will collect both DEX and MDB data using a combination of ad-hoc scheduling and trigger based events. Data collected by Glaux will be subsequently transferred to a handheld computer which, in turn, will communicate the information to the VendCast host application.

2 Related Documents

The following documents contain information supporting this requirements document:

- **ED-1:** *Audit Device – Conceptual Design Review*, Erin Defosse, 28 March 2002
- **ED-2:** *VendCast Java Agent 2.0 MRD-1.02*, Erin Defosse, 9 July 2001
- **ED-3:** **Glaux PRD Overview v1.0**, Erin Defosse & Alan May, XX Nov 2002
- **ED-4:** **Glaux PRD v1.0**, Erin Defosse & Alan May, XX Nov 2002
- **ED-5:** **Glaux LED Specification v1.0**, Erin Defosse, XX Nov 2002
- **BG-1:** **Glaux Access Control Use Cases, v1.0**, Bryan Godwin, 8 October 2002
- **EVA-DTS:** *EVA-DTS, Release 5.0*, European Vending Association
- **MDB/ICP:** *MDB/ICP, Version 2.0*, NAMA, 4 October 2000
- **EVS:** *Electronic Vending Standard (EVS) 3.0*, The Coca-Cola Company
- **DEX/UCS:** *Uniform Communications Standards for Direct Store Delivery – Implementation and User Guide (UCS/DSD-IUG)*, Uniform Code Council

3 Scope

This document explains the release objectives, high-level market requirements, critical milestones, and all responsible parties involved in defining, developing, and delivering this project in a timely manner.

Product Requirements DocumentProject: Glaux 2.0

4 Project Overview

The purpose of the Audit Device, or Glaux, initiative is to provide a low cost alternative to the on-line collection of vendor DEX and MDB data and to enable additional value-added capabilities at the vending machine such as the ability to control and audit an electronic lock that can open and close the machine. Glaux will be required to function as part of an integrated system in conjunction with PocketPC applications, the VendCast back end host, and an electronic lock.

5 Product Architecture

5.1 Solution Architecture

Figure 6.1.1 illustrates the solution architecture selected for addressing the Market Requirements. The solution consists of placing an embedded processor (Audit Device) inside the vending machine operable to obtain DEX data from the VMC and MDB data being generated by the VMC and the payment peripherals on-board the vendor. The DEX and MDB data is archived in non-volatile memory. Furthermore, the processor is interfaced to an electronic lock. The processor can command the lock to open and close by supplying appropriate power to the lock and, optionally, a digital control signal. A PocketPC based handheld can communicate with the Audit Device using Bluetooth RF communications. To enable this capability the Audit Device and the handheld are equipped with Bluetooth transceivers. When a handheld with the appropriate software interfaces with the Audit Device over Bluetooth, the DEX and MDB archives are transferred on-demand to the handheld. In addition, the handheld sends a command to the Audit Device that instructs it to open or close the electronic lock. All open and close events are also stored in a log on the Audit Device. This log can also be downloaded to the handheld.

The handheld is subsequently interfaced with the VendCast host application and data downloaded to and from it using any number of syncing or data transfer mechanisms. The VendCast host will use the collected data.

Product Requirements Document

Project: Glaux 2.0

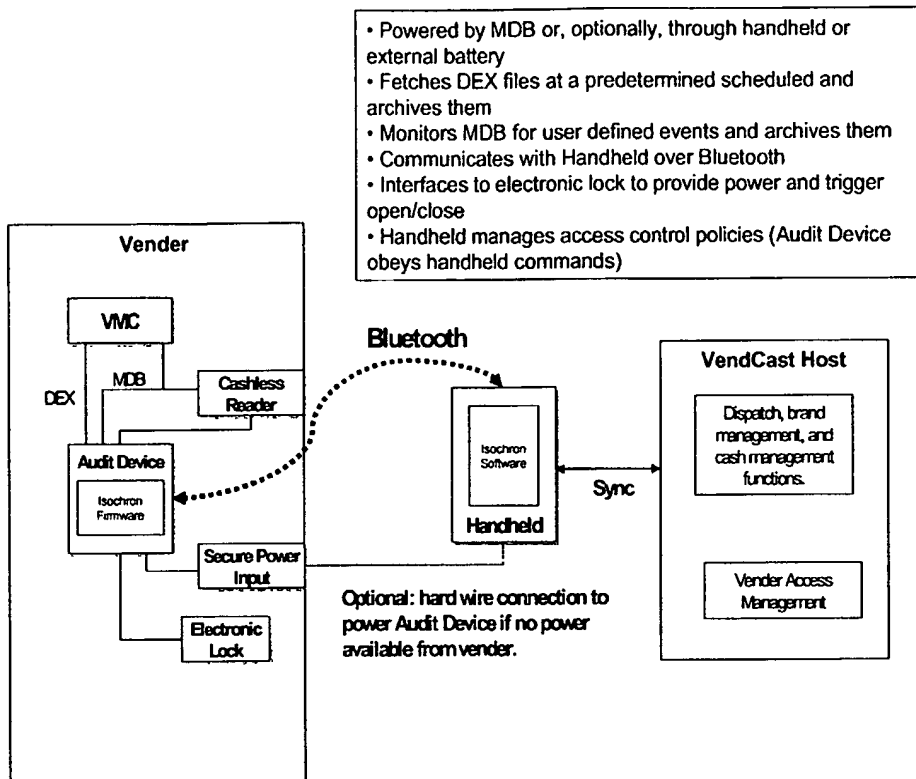


Figure 6.1.1: Solution Architecture

5.2 Hardware Architecture

In order to implement the solution architecture as presented herein, the Audit Device must support a variety of interfaces and internal subsystems. A diagram illustrating the hardware elements necessary for the implementation of these interfaces and subsystems is presented in **Figure 6.3-1**.

Product Requirements Document

Project: Glaux 2.0

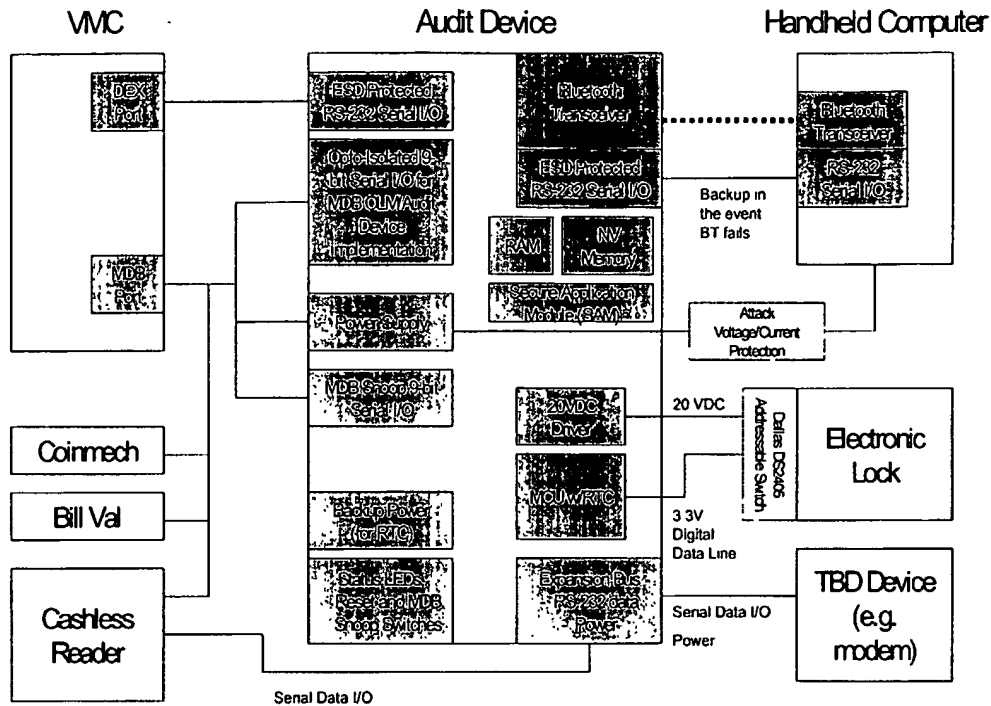


Figure 6.3-1: Hardware Architecture (All Functionality Implemented)

5.2.1 DEX Interface

The DEX Interface is an RS-232 serial data I/O interface that will be used to obtain DEX data from the vendor's VMC. The interface must provide ESD protection as well as deal with the various real-world implementations of DEX in vending machines. For example, the interface must be able to handle Master, Slave, and Slave-Read Only VMC's in software and, in hardware, be able to go in and out of a very high-impedance mode so that VMC's that attempt to detect devices connected on their VMC port cannot detect the Audit Device when it is not collecting data from the VMC.

5.2.2 MDB Interface

The MDB Interface is a serial data I/O interface that will be used to obtain atomic level sales transaction data as well as payment peripheral status data (e.g. error codes, aborted sales transactions, etc.). The MDB interface will be designed to operate in three modes: MDB Snoop, MDB Comms Gateway, and MDB Audit Device.

Product Requirements DocumentProject: Glaux 2.0

The MDB interface is implemented in hardware using an opto-isolated circuit design or an equivalent design that provides for very high transient protection to the Audit Device. In addition, reading and writing data over the MDB will require the Audit Device to implement 9-bit serial data which is non-standard. To guard against any unexpected incompatibilities with MDB Snoop (note: Snoop is not part of the MDB specification) the Audit Device shall implement both hardware and software level switches to turn MDB Snoop on/off.

5.2.3 PAN (Handheld Interface)

The Personal Area Network, of PAN, provides a mechanism for getting and setting data to and from the Audit Device using a handheld computer. The solution architecture calls for this interface to be implemented using Bluetooth RF, however, a backup wired RS-232 connection will be provided to guard against failure of the Bluetooth communications.

From a software perspective the PAN will be implemented as a Master-Slave where the handheld is the master and the Audit Device is a slave. A simple command-response protocol shall be implemented to allow the handheld to get and set data to and from the Audit Device.

The PAN will implement the security features inherent to Bluetooth hardware. These include device PINs and data encryption. For the RS-232 and IrDA interfaces, security will encompass only an access password given that the interfaces themselves are secure by virtue of the fact that they are located inside the vending machine itself.

5.2.4 Electronic Lock Interface

The Electronic Lock Interface allows the Audit Device to command an electronic lock on the vendor to open or close. The interface is implemented using a 4-wire interface: 20VDC power line to drive operation of the electronic lock, a power GND line, a 3.3V TTL level digital data line, and a data GND line. The TTL data line is used to command the lock to open and close as required.

The digital data line is used to communicate with Dallas Semiconductor 1-Wire addressable (part number DS2405). The 1-Wire switch is addressable using a unique 48-bit key. To command the electronic lock, the Audit Device must address the switch with the correct 48-bit key. Failure to provide the correct key would result in the command being ignored by the switch.

5.2.5 Expansion Bus

The Expansion Bus is designed to provide a means for the Audit Device to interface directly with other hardware that may eventually be available. For example, a WWAN radio transceiver, a WLAN transceiver, a Cashless Reader, etc.

The bus will implement RS-232 serial I/O and also provide output power sufficient to drive a typical WWAN or WLAN transceiver.

The Expansion Bus may accommodate more than one physical RS-232 port by implementing port multiplexing as necessary.

5.2.6 Power Subsystem

The Power Subsystem is responsible for providing operational power to all electronics on the Audit Device. Power to drive the operation of the unit will be obtained via the MDB interface and, as such, appropriate power regulation and surge suppression must be provided in order to deal with the transient fluctuations that occur on MDB.

Compatibility with electromechanical vendors will be provided through an external power converter/conditioner that will take 110VAC and/or DC or AC power from the vendor's peripheral bus (e.g. MicroMech) and convert it to 24VDC. A 6-pin "MDB" connector will be provided on the external power converter to allow the Audit Device to connect to it and draw power.

To deal with vendor power failures that would otherwise make it impossible to open the vendor, an optional interface to provide power to the Audit Device will be made available. This interface will consist of a contact point externally available on the vendor together with surge suppression and power conditioning hardware to guard against vandal attacks (e.g. Tazer guns, etc.). Once the Audit Device is powered, the handheld can command it to open the door via Bluetooth.

5.2.7 Data Storage Subsystem

The Data Storage Subsystem provides for non-volatile storage for data obtained via the DEX, MDB, and Handheld interfaces. For example, DEX files, MDB peripheral status, Audit Device configuration, POC data, etc.

A Secure Application Module will be provided in hardware to securely store the encryption keys necessary to implement the Glaux Security model. The SAM shall be in the form of a secure microprocessor or a secure EEPROM.

5.2.8 Timing Subsystem

Product Requirements DocumentProject: GlauX 2.0

The Audit Device must be able to maintain a RTC synchronized to a reference standard so that it can timestamp archived data. As such, backup power must be provided in a way that allows the Audit Device to maintain its clock even during extended vendor power down conditions.

5.2.9 Processor Subsystem

The Processor Subsystem consists of the embedded microprocessor and associated RAM necessary to drive the software and hardware functionality on the Audit Device.

5.2.10 User Interface Subsystem

The User Interface Subsystem on the Audit Device will consist of LED indicators on the unit which will provide core operational status feedback to the user, a reset button, and an MDB Snoop On/Off switch. Details regarding the number and function of the LEDs are presented later on in this document. A secondary UI Subsystem will be made available in software through the PocketPC handheld.

6 Software Architecture

The Audit Device must implement the necessary software functionality in order to meet the Market Requirements. The requirements are primarily data driven, that is, that collection, maintenance, and delivery of data is the primary objective of the Audit Device. As such, the software architecture has been developed using an Information Architecture as its source model. Specific functionality required for the Audit Device is derived by examining the various Use Cases of the system. The Information Architecture as well as key Use Cases are presented below.

6.1 Information Architecture

The Audit Device is part of data driven solution for our customers. The primary objective of the Audit Device is to collect, maintain, archive, and deliver data regarding the operation of a vendor over time. The specific types of data objects necessary to meet the Market Requirements are:

6.1.1 DEX Audit Data

DEX Audit data consists of the combination of archived DEX audit objects and the most current DEX audit object. A DEX audit object consists of the a) the DEX file obtained from the VMC, b) the GMT timestamp associated with

Product Requirements Document

Project: GlauX 2.0

the DEX file (the date and time at which the file was obtained from the VMC), and c) a Status field indicating the condition of the DEX Interface at the time that the audit attempt was made.

The status field shall indicate if the DEX Interface was in a "normal" state (meaning that the Audit Device is capable of retrieving DEX files) or if it is a "not communicating with VMC" state (meaning that the Audit Device is unable to communicate with the VMC and retrieve a DEX file). Additionally, if possible, a "not communicating with VMC" status should be expanded to include the exact reason behind the communications failure. Examples of such failures include a) bad DEX session password, b) timing failure at the protocol level, c) no response from VMC after initial session inquiry (0x05), or d) some other protocol level failure.

6.1.1.1 Current DEX

A Current DEX object is generated on demand by a request from the handheld computer and, as such, represents the most current DEX audit object available at the time that the request was generated by the handheld. Every time a Current DEX is requested and delivered to the handheld it will be added to the Archived DEX collection.

6.1.1.2 Archived DEX

Archived DEX consists of a collection of DEX audit objects which have been collected over a period of time by the Audit Device, including any Current DEX objects collected on demand by the Audit Device. The objects which make up archived DEX are collected based on a predetermined schedule programmed on the Audit Device. The schedule can consist of any combination of collection frequencies (e.g. every day at 20:00 hours) or any number of ad-hoc schedules (e.g. Monday at 12:00 and Thursday at 14:00).

The Archived DEX data shall be stored on the Audit Device in non-volatile memory in a compressed format. A ZLIB with Dictionary compression algorithm will be used in order to minimize the amount of non-volatile memory needed to store the archive. This data is to be delivered on-demand to the handheld.

Once the handheld downloads records from the archive these records shall be marked as "read" and will not be sent to the handheld on subsequent downloads unless specifically requested by the handheld. In the event that the size of the archive exceeds the physical memory allocation provided for it, the archive will act as a FIFO buffer whereby the oldest (based on timestamp) records are removed in order to make room for new ones. At any time the handheld will be able to

command to Audit Device to delete any single record or group of records.

6.1.2 MDB Audit Data

MDB Audit Data consists of a variety of different information elements which can be obtained by either listening in on the MDB using MDB Snoop. In MDB Snoop, the Audit Device will listen to communications being carried on both MDB data lines (VMC transmit and VMC receive) and examining the contents of the data being communicated between the VMC and MDB peripherals. For VMC's supporting the MDB Comms Gateway specification, audit data will be gathered using that service.

6.1.2.1 Current Peripheral Status

Current peripheral status refers to the operational status of the peripherals currently installed on the vendor's MDB. Examples of peripherals include bill validators, coin mechanisms, card readers, etc. The status of each of these peripherals can be determined by using MDB Snoop mode examining the history of the responses by the peripherals to the Poll command routinely sent to them by the VMC on the bus. Typically a peripheral will respond with a "normal" status response but, in the event of a problem with the peripheral, will respond with one of many different error codes documented in the MDB/ICP spec. Furthermore, it is important to note that peripherals are required to only transmit these detailed error codes once immediately after the error occurs, with subsequent responses to the STATUS command being a generic "peripheral disabled" response. Therefore, it is necessary for the Audit Device to track not only the current response to the Poll command but to also record the detailed error code and GMT timestamp associated with the original error event.

6.1.2.2 Peripheral Status Change History

Peripheral Status History is an archive of all MDB peripheral status events that have been recorded by listening in on the MDB. This archive consists of a series of GMT timestamped status change events. By timestamp and recording the peripheral ID (e.g. the type of peripheral as defined in the MDB/ICP spec) and every status change reflected in the device's response to the VMC's Poll command it is possible to construct a complete history of the status events that have occurred. This history must be archived in non-volatile memory and

Product Requirements DocumentProject: Glaux 2.0

transmitted on-demand to the handheld computer. The handheld computer can then analyze the history as needed.

6.1.2.3 Sales Transaction History

The Sales Transaction History consists of a series of GMT timestamped sales transactions which represent the complete set of successful and aborted vends at the vendor. These events can be tracked through MDB Snoop.

The Sales Transaction History will be transmitted on demand to the handheld computer.

6.1.2.3.1 Successful Vends

The Audit Device will be able to monitor transactions on the MDB to determine when a successful vend has occurred. The Audit Device will store the timestamp, sales value, and identify the peripheral(s) that provided the credit.

6.1.2.3.2 Exact Change Aborted Vends

Exact Change Aborted Vends are those vends that are aborted by the VMC due to an exact change condition at the vendor. That is, a bill validator transaction which was rejected by the VMC because there was no change available in the vendor to proceed with the vend. This event can be identified by noting when the bill validator places a cash escrow value on the VMC in response to the VMC's Poll command and the VMC immediately orders the bill validator to return the bill using the Escrow command.

Once the handheld downloads records from the archive these records shall be marked as "read" and will not be sent to the handheld on subsequent downloads unless specifically requested by the handheld. In the event that the size of the archive exceeds the physical memory allocation provided for it, the archive will act as a FIFO buffer whereby the oldest (based on timestamp) records are removed in order to make room for new ones. At any time the handheld will be able to command the Audit Device to delete any single record or group of records.

6.1.3 Time

The Audit Device will maintain an internal clock that is synchronized to GMT date and time. The Time on the Audit Device will be synchronized with GMT date and time available on the handheld computer every time that the

Product Requirements Document

Project: GlauX 2.0

handheld interfaces with the Audit Device. The handheld will be able to read the date and time on the Audit Device on-demand in order to validate it.

This Time will be used to date and timestamp all recorded events such as DEX Audit objects, MDB audit events, etc.

6.1.4 Audit Device Information

6.1.4.1 Asset Data

The Audit Device will maintain the asset data necessary in order to support the field management of the unit. This data will consist of the Audit Device serial number, model number, hardware revision number, manufacture date, and firmware revision number and date.

6.1.4.2 Configuration Data

The Audit Device will maintain a set of internal configuration parameters necessary for the operation of the device. These configuration parameters will include the DEX audit schedule, detailed DEX Interface parameters (e.g. packet timeout, character timeout, VMC type detection mode, VMC type list, etc.), an MDB audit event trigger table, etc. Detailed information on the various configuration parameters is found later in the detailed requirements section of this document.

6.1.4.2.1 Installed Flag

A key configuration parameter managed by the handheld (set operation) is the Installed Flag. This parameter is Boolean and defines the operating mode of the Audit Device. If set to False, then the Audit Device will turn off ALL link level (Bluetooth) and application level security functions in order to allow any handheld to connect to the Audit Device and perform set up. Once the flag is set to true, all link level and application level security functions are activated and only authenticated and authorized handhelds are allowed access to the device. Thus, a Bluetooth PIN is required for link level handshaking and an access certificate is required for application level. Furthermore, once the flag is set to true, it can only be set back to false via a hard reset of the unit or an authenticated command using a valid access certificate.

6.1.4.2.2 Has_Dex_Port Flag

Product Requirements Document

Project: Glaux 2.0

Specifies whether to indicate a VMC red failure to the user via the on-board LED. If set to "True" then a DEX read failure will be indicated on the LED per the Glaux LED Spec. If set to "False" then the Audit Device will make not attempt to read DEX.

6.1.4.2.3 Lock_Installed Flag

Specifies whether or not an electronic lock is physically installed with the Audit Device. If a lock is not physically present then no attempts are made to "unlock" the electronic lock. Furthermore, this flag causes the E-Lock LED on the Audit Device to indicate, per the Glaux LED Spec, that no lock is present rather than a failure to detect a lock.

6.1.4.3 General Events

The Audit Device will timestamp general events which occur at the unit. General Events include power on/off events, firmware upgrade events, etc. Detailed information on the various events that must be logged can be found later in the detailed requirements section of this document. Once the handheld downloads records from the log these records shall be marked as "read" and will not be sent to the handheld on subsequent downloads unless specifically requested by the handheld. In the event that the size of the log exceeds the physical memory allocation provided for it, the archive will act as a FIFO buffer whereby the oldest (based on timestamp) records are removed in order to make room for new ones. At any time the handheld will be able to command to Audit Device to delete any single record or group of records.

6.1.4.4 Handheld Transaction Log

The Audit Device will maintain a log of all transactions conducted between it and the handheld. Once the handheld downloads records from the log these records shall be marked as "read" and will not be sent to the handheld on subsequent downloads unless specifically requested by the handheld. In the event that the size of the archive exceeds the physical memory allocation provided for it, the archive will act as a FIFO buffer whereby the oldest (based on timestamp) records are removed in order to make room for new ones. At any time the handheld will be able to command to Audit Device to delete any single record or group of records.



Product Requirements Document

Project: GlauX 2.0

6.1.5 Ad-Hoc Data

The Audit Device will provide non-volatile memory storage space so that the handheld can write, delete, and read ad-hoc data as required. It will be up to the handheld to manage the storage space associated with the Ad-Hoc Data. The Ad-Hoc Data storage space may be used, amongst other things, to store a data structure (e.g. XML) containing information such as the vending machine asset information, space-to-sales information, selection and sku information, etc.

6.1.6 Ad-Hoc DEX Write

The Audit Device will implement two mechanisms for performing Ad-Hoc DEX Writes to the VMC.

6.1.6.1 Audit Device Managed DEX Write

The only DEX writes that will be managed by the Audit Device are those that are required to perform basic DEX extraction from the VMC. This includes:

6.1.6.1.1 DEX password writing

6.1.6.1.2 DEX error clearing

6.1.6.2 DEX Pass-Through

The Audit Device will provide a pass-through mode that will allow the handheld to establish a direct serial I/O communication session with the VMC. In this mode, the handheld will be able to engage in any type of DEX session directly with the VMC. This includes not only DEX writes but reads as well.

6.1.7 Electronic Lock Data

6.1.7.1 E-Lock Access Log

The Audit Device will maintain a log of electronic lock open and close events. The minimum data that will be logged at each open and close event is described below.

6.1.7.1.1 Driver ID (Employee ID)

Unique ID of the employee utilizing the handheld during the communication session with the Audit Device.



Product Requirements Document

Project: Glaux 2.0

6.1.7.1.2 Handheld ID

Unique ID associated with the PocketPC handheld communicating with the Audit Device for the purpose of perform an electronic lock function.

6.1.7.1.3 GMT Timestamp (Date and Time of event)

The Audit Device will tag all access event records with a GMT date and timestamp.

6.1.7.1.4 Access Status

Logs the result of the lock open/close command provided by the handheld (e.g. if an incorrect lock ID was provided then the lock open attempt fails)

6.1.7.2 Electronic Lock Access Key

The unique key code of the electronic lock. This is a unique 48-bit key that is preprogrammed into the Dallas Semiconductor addressable switch at the time the chip is manufactured. The electronic lock access key is obtained through direct interrogation of the lock using the 1-Wire data protocol.

6.1.8 Bluetooth Data

6.1.8.1 Bluetooth MAC Address

Every Bluetooth transceiver is factory programmed with a globally unique 6 byte MAC address. The MAC address can be obtained from the Bluetooth transceiver through an appropriate Bluetooth protocol stack API command. This MAC address shall be made available on demand to the Handheld.

6.1.8.2 Bluetooth Device Name

Every Bluetooth device has the ability to maintain a canonical name. This name is assigned programmatically by the application software. The Bluetooth Device Name associated with the Audit Device will be the unique Asset ID of the vendor in which it is installed. The Outlet ID is obtained automatically by the Audit Device from DEX data obtained (ID1 record) from the vendor's VMC. The Bluetooth Device Name will be set to the Asset ID using the appropriate Bluetooth

Product Requirements DocumentProject: GlauX 2.0

protocol stack API call. If an Asset ID is not available from the VMC/DEX, the Audit Device will default to the devices unique manufacturing serial number prefixed by the characters "HIAD" as its Bluetooth name. If that value is not available then the Audit Device will use the Bluetooth MAC address prefixed by the characters "HIAD".

6.1.8.3 Bluetooth PIN

The Bluetooth communications interface on the Audit Device will be secured using the built-in Bluetooth security schemes using a 16-byte (128-bit) PIN as well as the derived Link and Encryption keys. The Audit Device agent software is responsible for providing the PIN to the Bluetooth stack used in the implementation.

Details regarding the security model implemented on the Audit Device can be found in the GlauX Security PRD [ED-3].

6.1.9 Encryption Keys and Domain Hierarchy

Product Requirements Document

Project: GlauX 2.0

The Audit Device will securely maintain a set of 128-bit AES encryption keys to be used for authentication of digital signatures and the encryption of sensitive data using the AES encryption algorithm. The keys must be stored securely within the Audit Device to prevent them from being discerned through direct probing of the hardware by an unauthorized third party. Ideally, a secure microprocessor or EEPROM in hardware will be provided to securely store the keys.

In addition to the encryption keys, the Audit Device will maintain a Domain Hierarchy stored in non-volatile memory. The Domain Hierarchy defines the trust hierarchy that will be used to authenticate handheld devices attempting to communicate with the Audit Device as well as to enforce security policies tied to the agent's business logic.

Details regarding the Security model for the Audit Device can be found in the GlauX Security PRD document [ED-3].

6.1.9.1 Agent AES Key

The Audit Device will maintain a 128-bit AES encryption key which is unique to the particular Audit Device and logically tied to its serial number. The Agent Key will be loaded at manufacture using a secure process.

6.1.9.2 Root Domain AES Key(s)

The Audit Device will maintain one or more "global" 128-bit root domain AES keys. These encryption keys are used to encrypt/decrypt data sent/received to and from the handheld. The Root Domain key(s) will be loaded at manufacture using a secure process.

6.1.9.3 Agent Public/Secret Key Pair

The Audit Device will maintain a PKI key pair in non-volatile memory. The key pair will be generated dynamically by the agent software or loaded at manufacture using a secure process. The key sizes will be at least 1024 bits.

6.1.9.4 Host Public Key

The Audit Device will maintain the PKI public key for the host application in non-volatile memory. The key size will be at least 1024 bits.

6.1.9.5 Domain Hierarchy

The Audit Device will maintain a domain hierarchy in non-volatile memory. The Domain Hierarchy consists of domain names and their hierarchical relationship. The Domain Hierarchy is provided to the Audit Device by the handheld after installation using a secure process. The Domain Hierarchy

Product Requirements Document

Project: GlauX 2.0

provided by the handheld is digitally signed by the host using its PKI secret key and validated by the agent software using the host's PKI public key.

The data objects and the flow of information into and out of the Audit Device are depicted graphically in the information architecture diagram presented in **Figure 7.1-1**. The diagram specifically notes which elements of the solution are responsible for GET and SET operations related to the data.

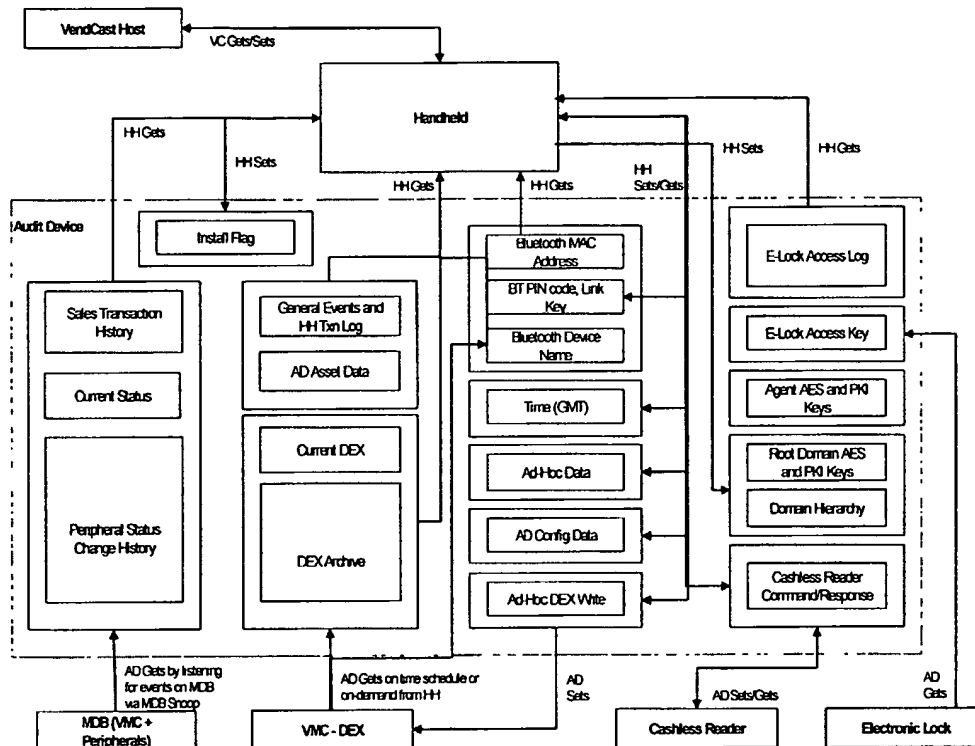


Figure 7.1-1: Information Architecture

The estimated total amount of non-volatile memory required to store the data objects presented above is around 400KB. This includes a 50% factor of safety in the calculations, does not include the Ad-Hoc data objects, and assumes that audit data represents 60 days of vendor activity and that a DEX object is created and archived 4 times per day. Using the VendCast 1.20 Firmware as a guideline, non-volatile storage of approximately 140KB plus a 50% factor of safety would have to be provided for firmware. This brings the total non-volatile storage requirements of the Audit Device to 600KB, not including Ad-Hoc storage. The amount of data storage available for Ad-Hoc storage would simply be allocated based on whatever is left after the appropriate non-volatile memory chips are selected.

Product Requirements Document

Project: Glaux 2.0

6.2 PAN Network Architecture (Bluetooth)

The Audit Device will act as a slave node on the PAN while the PocketPC handheld acts as a Bluetooth master. Figure 7.2-1 illustrates the master-slave relationship under various topologies. Topologies (a) and (b) will be supported in Phase 1 development.

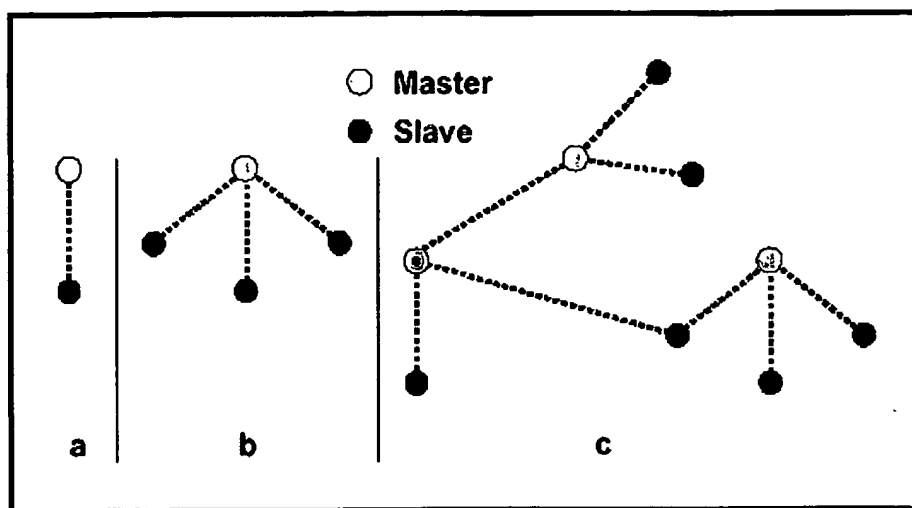


Figure 7.2-1: Bluetooth PAN Topologies

6.2.1 Audit Device Inquiry

The Audit Device will support Bluetooth device inquiry. It shall make its presence known on the PAN to any Bluetooth capable device that inquires about its presence. The inquiry process will provide the MAC address and the Bluetooth Device Name to the inquiring device.

Even though the Audit Device will be enquirable, the ability to connect to it will be restricted by implementing both link level Bluetooth security as well as application level security.

Phase 2 development may impose stricter guidelines regarding enquirability.

6.2.2 Service Discovery

The Audit Device will not make its services discoverable to a connected Bluetooth device. This improves the security of the system by obscuring the entry points into the Audit Device to any unauthorized third party.

Product Requirements Document

Project: Glaux 2.0

6.3 Security Architecture

The Audit Device will implement two layers of security, one at the application level and the other at the communication link level using Bluetooth security.

6.3.1 Link Level Security

The Audit Device will implement all of the security features available via the Bluetooth protocol stack. Specifically, the Audit Device will make use of the device authentication, service authentication, and data encryption capabilities found in Bluetooth. The Bluetooth capabilities provide link level security to ensure that:

- 1) Only authenticated Bluetooth devices are able to connect to the Audit Device
- 2) Only authenticated Bluetooth devices with the appropriate privileges are granted access to the services provided by the Audit Device
- 3) The information communicated between the authenticated device and the Audit Device is performed over a secure encrypted channel that can not be monitored by a third party

6.3.2 Application Level Security

In addition to link level security the Audit Device will implement a second layer of security at the application level. This layer of security will provide the following capabilities:

- 1) Encryption of sensitive data payloads using 128-bit AES encryption
- 2) Authentication using digital certificates based on PKI infrastructure

Details regarding the security implementation on the Audit Device can be found in the Glaux Security PRD [ED-3, ED-4].

6.3.3 Key Management

Key Management must be invisible to the customer and will be enabled to occur automatically during normal communication sessions. For example, if a particular link level Bluetooth key is compromised, the driver handhelds will be programmed to perform key changes on all devices that they come in contact with. Fundamentally, key management will be performed by the PocketPC handheld and the VendCast host. However, the Audit Device must implement the proper authentication and screening process to ensure that the

Product Requirements Document

Project: Glaux 2.0

handheld attempting to modify a security key, is a valid and authenticated handheld.

Details regarding the security implementation on the Audit Device can be found in the Glaux Security PRD [ED-3].

6.4 Business Logic – Use Cases

The business logic implemented on the Audit Device shall satisfy the Use Cases defined herein. Additional use cases and market requirements are contained in the Glaux Access Control Use Cases [BG-1] document.

6.4.1 Installation without Handheld

NOT SUPPORTED

6.4.2 Installation with Handheld

Installation of the Audit Device on the vendor may occur in the field or in the bottler's cooler shop. This task is expected to be performed by a person with technical skills and trained in the installation of the Audit Device. This installation process **REQUIRES** that a handheld with software operable to configure the Audit Device be present in order to perform a complete installation.

- 1) The Audit Device is physically mounted inside the vending machine
 - a. Power to the vendor door is shut off or power to the entire vendor is removed.
 - b. The Audit Device's DEX harness (phono plug) is inserted into the DEX port for the VMC
 - c. The Audit Device's MDB harness is attached to the MDB.
 - a. The Audit Device is connected to the electronic lock
 - b. Any expansion peripherals are connected to the Expansion Bus.
 - c. User will depress and hold the reset button and restore power to the vendor door (or vendor itself). This will cause power to flow through the MDB and turn on the Audit Device.
 - d. Optionally, a handheld is connected directly to the Audit Device using its RS-232 handheld interface. If connected over RS-232, the Audit Device can audit the entire installation process. The Audit Device presents detailed system diagnostics and provides for low level configuration control using the handheld interface.
 - e. At power up the Audit Device will first perform a self-diagnostic. If the self-diagnostic fails (e.g. a memory parity error) then the Audit Device will light its LEDs as defined in the Glaux LED Specification [ED-5] to alert the user of the problem. If a problem

Product Requirements Document

Project: Glaux 2.0

is encountered the user may attempt to diagnose the issue with a handheld (e.g. download new firmware, soft reset the unit, hard reset the unit, etc.).

- f. After the unit is successfully booted the Audit Device will setup and establish communications as necessary over the PAN, DEX, MDB, Electronic Lock, and Expansion Bus interfaces.
 - i. Audit Device sets up the DEX Interface as necessary to manage DEX password, VMC Type detection, etc. as currently performed in the VendCast agent firmware (see ED-2).
 - ii. Audit Device initializes the PAN interface as necessary. In the case of Bluetooth this may include the initialization of a Bluetooth hardware module. The Audit Device sets the BT Name to the Audit Device's manufacturing serial number prefixed by the characters "HIAD". Later on during the install process, the PocketPC handheld is used to set a register on the Audit Device which will contain the Bluetooth Name to use after installation is complete. Nominally, this will be the customer assigned Asset ID of the vending machine.
 - iii. If using Bluetooth to communicate to the handheld, communication session with the Audit Device may be established by the handheld in order audit and manage the install process.
 - iv. Audit Device sets up MDB Interface as necessary to snoop on the MDB. In future releases, this set up will include registering the device on the MDB as an MDB Comms Module per the MDB/ICP specification and/or the EVS specification.
 - v. Audit Device inspects the Electronic Lock interface for the presence of an electronic lock. If one is detected, the unique 48-bit address of the lock is acquired and stored for use.
 - vi. LEDs on the Audit Device provide visual feedback on the status of the PAN, DEX, MDB, Expansion Bus, and electronic lock interface setup. The LEDs will operate per the Glaux LED Specification [ED-5]
 - vii. If a problem is detected by observing the LEDs or through inspection of the diagnostic data being presented by the handheld, the user can attempt to correct the issue through manipulation of the configuration parameters on the Audit Device with the handheld.
- 2) User uses the handheld to set up the basic configuration parameters of the Audit Device.
 - a. Initial Handshake (Bluetooth PAN)

Product Requirements Document

Project: Glaux 2.0

- i. When the unit is in an uninstalled mode (Install Flag = False) the handheld application is allowed full access to the Audit Device at the link level and application level.
 - ii. Once a session is established, the Audit Device proceeds to automatically synchronize its internal clock with the clock on the handheld. This routine synchronization provides the Audit Device with a reliable reference standard for which to run its RTC off of.
- b. Service tech then accesses the appropriate screen on the handheld application and programs a variety of basic configuration parameters and POC parameters on to the Audit Device.
 - i. Configure the DEX audit data collection schedule and update the MDB trigger table
 - ii. Set Vendor Asset, Selection, and S2S data on the vending machine's VMC.
 - iii. Store Ad-Hoc Data provided by the handheld
 - iv. PAN network parameters
 - v. Set the Lock_Installed flag
 - vi. Set the Has_DEX_Port flag
- g. The handheld application guides the installer through the following security setup requirements
 - i. Set the Asset ID associated with the vendor. This value will be used to define the Bluetooth name of the Audit Device once the configuration process is complete.
 - ii. Define the Route number and Outlet ID of the vendor.
 - iii. The handheld will push this data to the Audit Device together with a Domain Hierarchy initially provided by the host application. For more details please refer to the Glaux Security PRD.
- 3) The Audit Device logs all handheld activity in the Handheld Transaction Log
- 4) Once all configuration parameters are set the installer sets the Audit Device to an "Installed" mode. The handheld application, in turn, commands the Audit Device to set the Installed Flag = True. This causes all application level security functions to become active.

6.4.3 Audit (Steady State)

The Audit use case represents the steady state operation of the Audit Device once it has been installed, configured, and placed in the field with a live vendor. The Audit Device will perform automatic collection of DEX, MDB, and electronic lock Access audit data as defined by the DEX audit schedule information, the MDB event triggers programmed into it during the installation phase (or as defined by its default settings), and the electronic lock access events that occur from time to time.

- 1) AD follows pre-defined data collection configuration
 - a. DEX: at a given frequency (Daily, Weekly, etc.) at a certain time-of-day or on specified days of the week and at a specified time-of-day
 - b. MDB: based on user defined triggers such as a change in peripheral status, successful sales transactions, aborted sales transactions.
 - c. Access: whenever the AD receives a command from the handheld to open the electronic lock it will log the event. If the information is available, the AD will log the success or failure of the access attempt.
 - d. As data is collected it is timestamped and stored/archived into non-volatile memory.
- 2) If a power outage occurs, the Audit Device must maintain the audit data and its RTC alive for up to 3 months. In the event that the outage is longer then, when the unit comes back up, it will begin timestamping using time from boot-up. The handheld software can later attempt to deduce actual date/time – note: this only works for the data acquired after the last power cycle.
- 3) The data collected during the audit phase corresponds to the data elements defined in the Information Architecture section of this document.

6.4.4 Driver Visit

The route driver will visit vendors on some frequency (variable or fixed) in order to deliver product and collect cash. Every time the driver visits a vendor s/he will, in addition to delivering product and collecting cash, use their route handheld to download audit information from the Audit Device, download cashless transaction data (if the AD is connected to a Cashless Reader), and upload any data needed to update the operations of the Audit Device, the vendor itself, or any peripherals that may be attached via its Expansion Bus (e.g. negative files for a Cashless Reader). Furthermore, a driver visit may be used to automatically upgrade firmware or security keys on the Audit Device.

At the end of the day, the route driver will interface their handheld to the VendCast host application and the information collected from all vendor's visited will be downloaded from the handheld to the host application. Similarly, data that needs to be pushed out from the VendCast host to the Audit Device (or attached peripherals) may be stored on the handheld at this point.

A route driver visit to a vendor will consist of the following steps:

Product Requirements Document

Project: Glaux 2.0

- 1) For the purpose of downloading the latest Audit Data on to his or her handheld, the route driver arrives at a location near the vending machine and accesses the route management application on the handheld. If the vendor appears in the daily itinerary and is Bluetooth enabled, the handheld will establish a communication session with the Audit Device. At this point the Audit Data can be downloaded and the driver may choose to issue a Door Open command to the Audit Device for the purpose of restocking the machine. The driver may also choose to modify the space to sales configuration of the vendor, etc.
 - a. Initial Handshake (Bluetooth PAN)
 - i. Audit Device and handheld handshake in order to discover each other at the Bluetooth (Link) Level. This handshake will require that Bluetooth PINs on both the Audit Device and handheld match. If they do, a secure (encrypted) Bluetooth session is established. For more details refer to the Glaux Security PRD.
 - ii. Once a Bluetooth session is established the handheld must present a valid Access Certificate to the Audit Device. The Audit Device will validate the certificate. If the validation fails, the handheld is denied access to the Audit Device. For more details refer to the Glaux Security PRD.
 - iii. Once a session is established, the Audit Device proceeds to synchronize its internal clock with the clock on the handheld. This routine synchronization provides the Audit Device with a reliable reference standard for which to run its RTC off of.
 - c. The handheld software drives the exact steps from this point on. From the Audit Device's perspective, the specific workflow being implemented is invisible. All it does is respond to commands it receives from the handheld, in whatever order it gets them. The commands supported by the Audit Device are derived from the Information Architecture presented earlier. These include:
 - i. For example, the handheld software commands the Audit Device to deliver all archived audit data as well as the most current DEX and MDB peripheral status data. To get the most current DEX, the Audit Device actively polls the VMC. The AD creates a Current DEX audit object and transmits it to the handheld. Alternatively, the handheld may request a DEX Pass-Through session and perform its own DEX extraction. Note that the handheld application is responsible for applying "refill" DEX tags, if necessary. Additional tasks that can be commanded include:
 - Configure the DEX audit data collection schedule and update the MDB trigger table
 - Set Vendor Asset, Selection, and S2S data on the VMC by using a DEX Pass-Thru operation.

Product Requirements Document

Project: GlauX 2.0

- Store Ad-Hoc Data: this is a catchall to enable future capabilities.
 - Soft reboot the Audit Device in an attempt to resolve a serial communications problem, for example.
 - Downloading of cashless transactions from a Cashless Reader on the Expansion Bus.
- ii. The Audit Device preserves all of the audit data after it has been downloaded to the handheld. The downloaded data is marked as "read" but not deleted from non-volatile storage. As the size of the audit archives increases the oldest data is overwritten with newer data (FIFO). During subsequent driver visits only non-delivered data is downloaded, unless the handheld application specifically requests that all data be downloaded. By only downloading the most recent data we can minimize the file transfer time from the Audit Device to the handheld. However, the handheld may request records regardless of their "delivered" status using an ad-hoc record query mechanism.
- 2) If needed, the user instructs the handheld to command the Audit Device to open the vendor's electronic lock by sending it a Door Open command. This opens the lock. The lock is energized into an open state for 10-seconds (nominal time). The lock automatically closes once the Audit Device stops energizing it. All lock access activity is logged in the Access Log.
- 3) The Audit Device logs all handheld activity in the Handheld Transaction Log

6.4.5 Service Tech Visit

A Service Tech will visit a vendor from time to time as service problems are reported by customers, route drivers, of the VendCast host application itself. The Service Tech will arrive at the vendor and, based on the type of problem reported, will attempt to diagnose the problems at the vendor. The Service Tech will have with him/her a PocketPC handheld that will allow him/her to communicate with the Audit Device for the purpose of allowing him/her to inspect the operational status of the MDB peripherals, the VMC, and the Audit Device itself and will attempt to correct any problems encountered. In some other cases, the Service Tech may be called upon to modify the configuration of the vending machine, the Audit Device, or any peripheral attached to the Audit Device's Expansion Port.

- 1) The tech will first inspect the status of the LEDs on the Audit Device to ascertain whether or not there is a reported problem. If any of the LEDs is displaying a problem condition the tech will take appropriate action.

Product Requirements Document

Project: Glaux 2.0

- a. If LEDs indicate that no power is present then the tech will attempt to reinstall the cabling or check the overall power condition of the vendor.
 - b. If LEDs indicate an interface problem (DEX or MDB) then the driver may choose to simply reboot the unit by power cycling it, resetting all cables, or proceed to use the handheld to diagnose the problem (see below). Please refer to the Glaux LED Spec for details on the LED meanings.
- 2) For the purpose of inspecting the detailed operational status of the Audit Device, the MDB peripherals, the VMC, the electronic lock or any peripheral attached to the Audit Device's Expansion Port, the tech will establish a communication session with the Audit Device using a direct connection over RS-232 or wirelessly via the Bluetooth PAN.
- a. Initial Handshake (Bluetooth PAN)
 - i. Same as in Driver Use Case.
 - b. Problem Assessment: the handheld prompts the service tech on the possible actions that can be taken at this point. The service tech may select to view the operational status of the VMC, the MDB peripherals, and the Audit Device itself. The details of the problem resolution workflow are managed by the PocketPC handheld. The Audit Device simply responds to commands given to it by the handheld.
 - i. For example, the handheld software may command the Audit Device to deliver all DEX, MDB, and Access audit data, General Events, Vendor Information, and Audit Device Asset Data. The DEX and MDB audit data downloaded is NOT marked as "read" in order to not interfere with the normal audit data collection process performed by route drivers.
 - ii. The MDB audit data is analyzed to determine the status of the peripherals and their status history.
 - iii. The General Events are analyzed to determine if any internal error conditions have been logged and to determine the power cycle history of the vendor/Audit Device.
 - iv. The DEX file is examined and its configurations (e.g. selection info, space-to-sales) compared with those stored in the Vendor Information data objects. If the Audit Device is unable to download a DEX file then this is also noted.
 - v. After the analysis of the data is complete the tech is presented with the results of the analysis. The tech can view the summary results or drill down on the history of, for example, an MDB peripheral's status over time.
 - c. At this point the tech can take action, as required, to correct any problems detected during the analysis of the data.

- i. Configure the Audit Device and/or the VMC (data collection schedules, DEX and MDB interface parameters, VMC programming, etc.).
 - ii. Soft or hard reboot the Audit Device. Note: hard reboot of the Audit Device will cause it to lose all its DEX and MDB data and require that the unit be "reinstalled" from a software perspective.
 - iii. Securely upload new firmware to the Audit Device
- 3) Other functions that may be carried out by the tech include:
 - a. View Handheld Transaction Log
 - b. Replace the Audit Device with a new one and perform the activities associated with the Install use case.
- 4) If needed, the user instructs the handheld to command the Audit Device to open the vendor's electronic lock by sending it a Door Open command. This opens the lock. The lock is energized into an open state for 10-seconds (nominal time). The lock automatically closes once the Audit Device stops energizing it. All lock access activity is logged in the Access Log.
- 5) Audit Device logs all activity in the Handheld Transaction Log

6.4.6 Interface with Cashless Reader

This Use Case for the Audit Device involves a situation where the Audit Device is installed inside a vendor together with an Isochron Cashless Reader. The Cashless Reader is a piece of hardware designed to enable the acceptance of non-cash payment tokens at the vending machine (e.g. credit card, Speedpass RFID, etc.). It is desired that, in this scenario, the single point of interface at the vending machine that was presented in the previous Use Cases, where the driver or tech had only to interface with one device, be maintained. In this setup, the Audit Device and the Cashless Reader are physically interfaced using the Expansion Bus on the Audit Device. A similar bus is assumed to exist on the Cashless Reader. The handheld interface on the Audit Device provides access to data on the Cashless Reader and allow the handheld to execute commands on the Cashless Unit. These capabilities may be provided by the Audit Device by using a Pass-Through mode to communicate with the Cashless Reader or through commands executed on the Audit Device that, in turn, cause the Audit Device to perform its own communication with the Cashless Reader.

The physical setup of this Use Case would require that the Audit Device and Cashless Unit be connected using a cable harness or mounted together at their expansion bus points. Both units would maintain their respective MDB connections.

6.4.7 Interface with WLAN/WWAN Transceiver (Radio Modem)

The Audit Device may be installed together with a WLAN or WWAN transceiver connected to its Expansion Bus. In this scenario, the WLAN or WWAN transceiver will act as another command/control interface point for the Audit Device, not unlike the Handheld Interface. The Audit Device will respond to remote commands provided to it over the WLAN or WWAN communications medium.

The Audit Device must be able to auto-configure any supported WLAN or WWAN transceiver attached to it. This means that the Audit Device must be able to perform at least the following operations:

- 1) Detect the presence of a transceiver on the Expansion Bus
- 2) Identify the type of transceiver present and select the appropriate communications protocol to command and control the transceiver
- 3) Initialize the transceiver to its appropriate settings
- 4) Detect the presence of the wireless network and report this information via the user interface (LEDs and/or handheld)
- 5) In the case of a WWAN transceiver, commission itself with the VendCast Host application, if not already commissioned.
- 6) In the case of a WLAN transceiver, establish a connection with the WLAN hub (if applicable)
- 7) Detect inbound commands arriving via the transceiver, validate/authenticate the commands, and reply to them using an appropriate communications protocol

6.5 Handheld and Audit Device Interaction

6.5.1 Master-Slave Relationship

Based on the Information Architecture and Use Cases presented, it is desirable that the handheld and Audit Device interact using a Master-Slave relationship where the handheld drives all workflow related functionality and the Audit Device simply exposes various methods and properties (data) to the handheld. This design approach allows for maximum flexibility in the system and makes the system more scalable given that modifications to the functionality can be made by upgrading the code on the handheld rather than requiring that every Audit Device be upgraded.

Under this type of architecture, a typical interaction between a handheld and the Audit Device is depicted in **Figure 7.3.1-1**. Note that the interaction diagram does not include any link level interactions that may occur during, for example, establishment of a communication session over the Bluetooth PAN.

Product Requirements Document

Project: GlauX 2.0

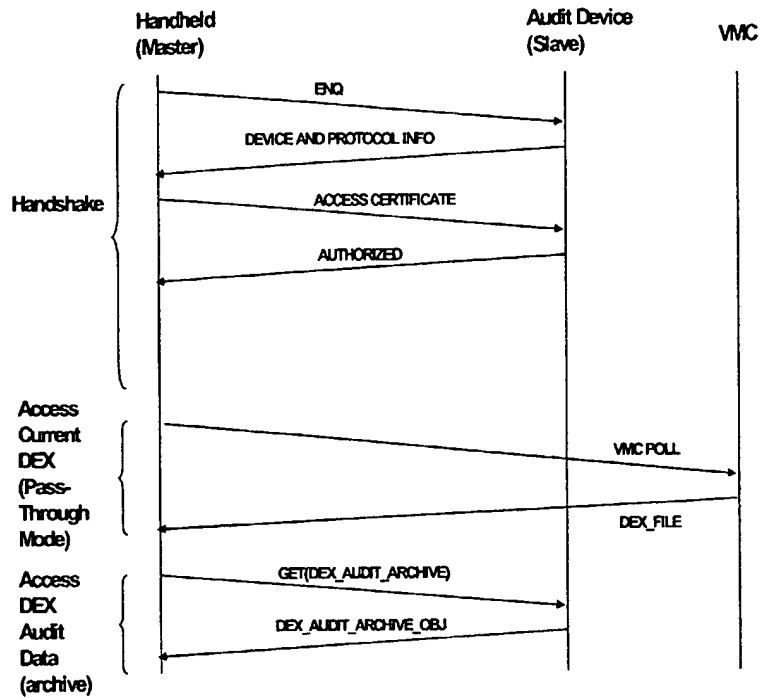


Figure 7.3.1-1: Sample Interaction Diagram

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning these documents will not correct the image
problems checked, please do not report these problems to
the IFW Image Problem Mailbox.**